

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
 «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**ОТЧЁТ**

**по лабораторной работе №10 «Настройка параметров мандатного управления доступом и мандатного контроля целостности»**

**по дисциплине «Защита в операционных системах»**

Выполнил: студент гр. ВКБ43

Ковалев Д. П.

Проверил:

доц. Скляров А.В.

г. Ростов-на-Дону

2025 г.

**Цель работы:** освоить администрирование основных параметров мандатного управления доступом и мандатного контроля целостности в ОССН с применением графических утилит и консольных команд.

**Задание 1.** Начать работу со входа в ОССН в графическом режиме с учётной записью с привилегированного пользователя (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»).

Зайдем от имени администратора в систему. Рабочий стол администратора представлен на рисунке 1.



Рисунок 1 – рабочий стол администратора системы

**Задание 2.** Запустить графическую утилиту редактирования учётных записей пользователей «Политика безопасности» через меню «Панель управления» главного пользовательского меню.

Запустим просто графическую утилиту “Политика безопасности”, её также можно открыть через пуск. Интерфейс данного приложения представлен на рисунке 2.

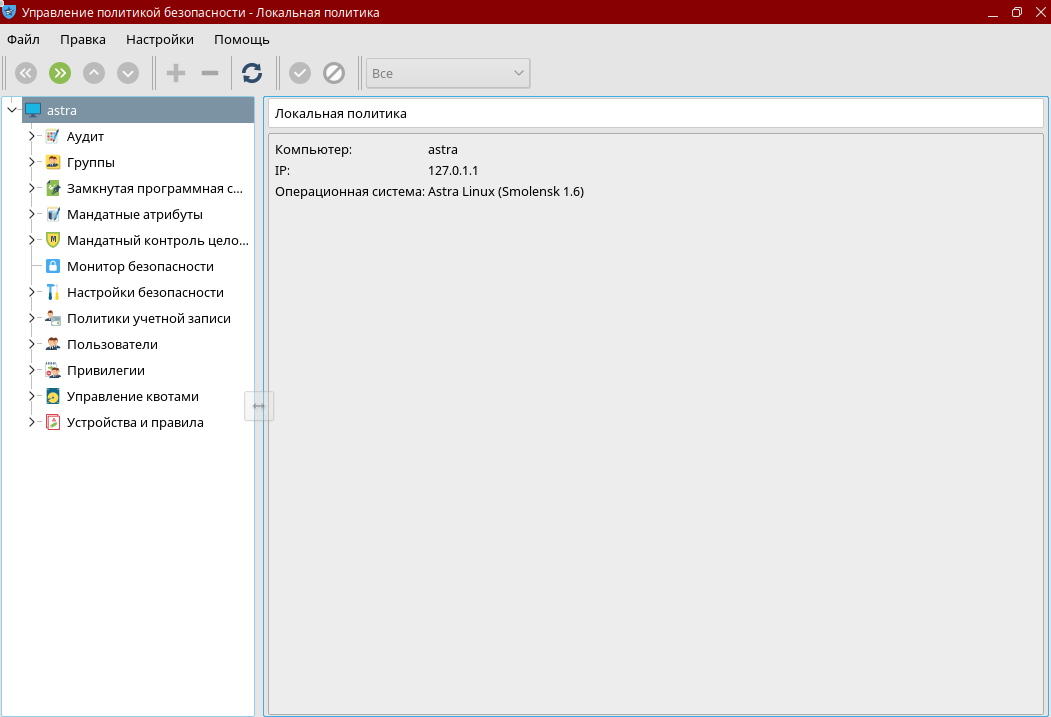


Рисунок 2 – управление политикой безопасности

**Задание 3.** Модифицировать параметры мандатного управления доступом, для этого осуществить следующие действия: открыть раздел «Мандатные атрибуты», «Уровни конфиденциальности» и выбрать «0»: Уровень\_0» и переименовать данный уровень доступа: «Уровень0». Выполнить создание уровня доступа с именем «Уровень \_4», задав значение равное 4, после чего проверить наличие записи «Уровень\_4» в списке «Уровни конфиденциальности». Выполнить обратное переименование: «Уровень0» в «Уровень \_0».

Для начала переименуем уровень. Выполнение данного пункта задания представлено на рисунке 3.

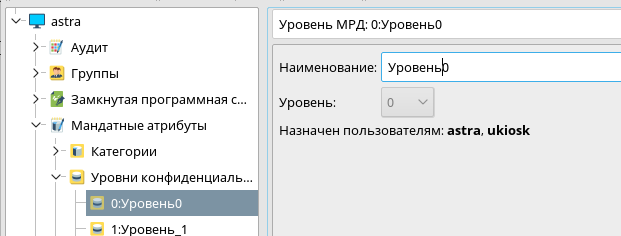


Рисунок 3 – изменение имени уровня

Теперь перейдем к созданию уровня. Для этого с помощью ПКМ нажмите на “Уровни конфиденциальности”, после этого получится создать новый уровень, как представлено на рисунке 4.

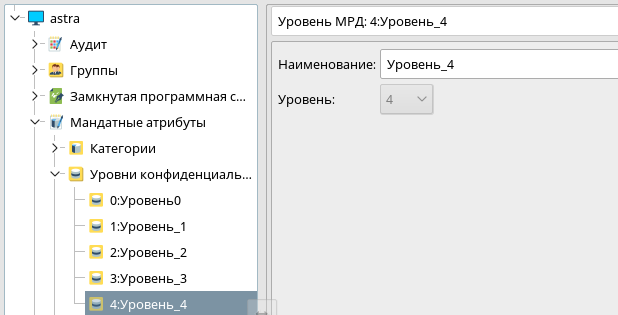


Рисунок 4 – создание нового уровня для задания

Теперь переименуем обратно на исходное название, как представлено на рисунке 5.

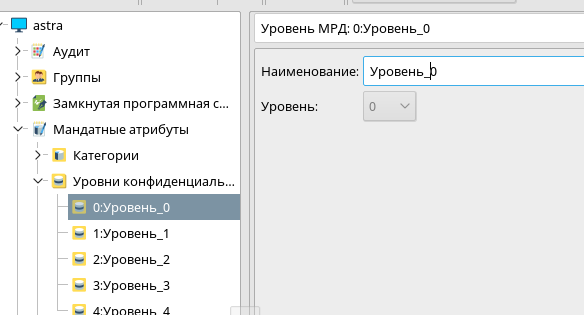


Рисунок 5 – переименование в исходное

**Задание 4.** Создать учётную запись пользователя user1, установив максимальный уровень доступа: «Уровень\_4».

Для выполнения данного задания также будем пользоваться графическим интерфейсом. Конфигурация представлена на рисунке 6.

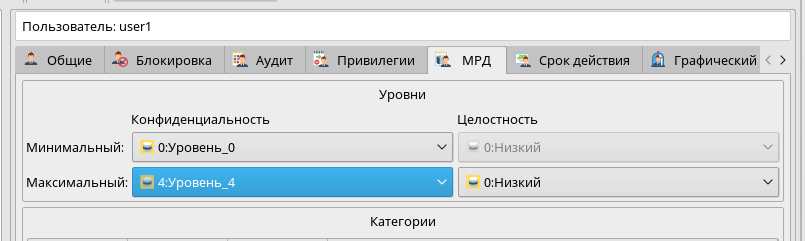


Рисунок 6 – создание новой учетной записи пользователя

**Задание 5.** Попытаться удалить уровень доступа 4 из раздела «Уровни конфиденциальности» путём выбора в контекстном меню пункта «Удалить». Объяснить результат.

Такое происходит по той причине, потому что у нас стоит максимальный уровень целостности. При удалении данной роли у пользователя user1 теряется кусок прав, которые мы до этого добавили. То есть появляется некая неопределенность, поэтому даже у администратора есть запрет на удаление данного уровня. Результат представлен на рисунке 7.

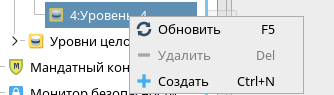


Рисунок 7 – невозможность удаления уровня

**Задание 6.** Вывести в терминал Fly параметры мандатного управления доступом для учётной записи пользователя user1. Для этого выполнить следующие действия. запустить терминал Fly и перейти в каталог /etc/parsec/macdb; прочитать параметры учётной записи user1 командой sudo cat /etc/parsec/macdb/XXXX (XXXX – UID пользователя user1). определить максимальный уровень доступа учётной записи user1 командой sudo grep "user1:" \* |cut -d: -f 5; Определить минимальный уровень доступа учётной записи user1 командой sudo grep "user1" \* |cut -d: -f 3 и проверить его соответствие данным, отображаемым в графической утилите «Политика безопасности». Создать неиерархические категории с использованием графической утилиты «Политика безопасности». Для этого выполнить следующие действия. В разделе «Категории» (Панель управления → Безопасность → Мандатные атрибуты → Категории) удалить исходные неиерархические категории; затем создать новую неиерархическую категорию с именем «Otdel1», «Разряд» - 0; в разделе «Категории» создать новые неиерархические категории: «Otdel2» («Разряд» — 1), «Upravlenie» («Разряд» — 2).

Для начала запустим терминал fly и перейдем в каталог /etc/parsec/macdb, как представлено на рисунке 8.



Рисунок 8 – переход в директорию /etc/parsec/macdb

Прочитаем параметры учетной записи, как сказано по условию задания. UID пользователя можем узнать через графический интерфейс. В результате получилось то, что представлено на рисунке 9. Файлы в директории /etc/parsec/macdb/ в ОССН Astra Linux содержат информацию о мандатных метках безопасности (уровнях доступа и категориях) для различных субъектов системы. Формат записи обычно следует паттерну: имя объекта : уровень целостности : минимальный уровень доступа : максимальный уровень доступа : категории доступа.

Уровень конфиденциальности (0) - определяет степень секретности информации, к которой имеет доступ пользователь. Уровень 0 означает достаточно высокий уровень доступа.

Минимальный уровень доступа (0) - определяет степень секретности информации, к которой имеет доступ пользователь. Уровень 0 означает достаточно высокий уровень доступа.

Максимальный уровень доступа (4) - определяет степень секретности информации, к которой имеет доступ пользователь. Уровень 0 означает достаточно высокий уровень доступа.

Битовая маска категорий (0) - определяет конкретные категории доступа в виде битовой маски.

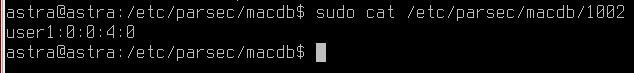


Рисунок 9 – просмотр мандатных меток безопасности

Определим максимальный уровень доступа учётной записи user1 командой sudo grep "user1:" \* |cut -d: -f 5. Результат представлен на рисунке 10.

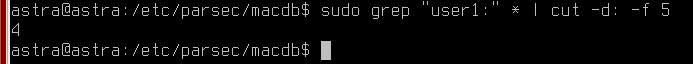


Рисунок 10 – максимальный уровень доступа

Определим минимальный уровень доступа учётной записи user1 командой sudo grep "user1" \* |cut -d: -f 3. Результат представлен на рисунке 11.

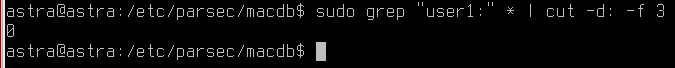


Рисунок 11 – минимальный уровень доступа

Теперь создадим неиерархические категории с использованием графической утилиты «Политика безопасности». Для этого нужно выполнить следующие действия: в разделе «Категории» (Панель управления → Безопасность → Мандатные атрибуты → Категории) удалить исходные неиерархические категории. В результате должно получиться то, что представлено на рисунке 12.

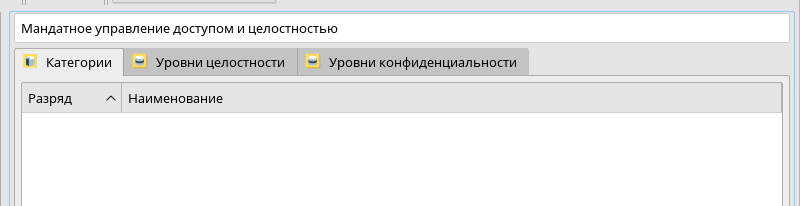


Рисунок 12 – удаление всех категорий

Теперь перейдем к созданию новой неиерархической категорию с именем «Otdel1», выставив «Разряд» - 0. Результат выполнения представлен на рисунке 13. Неиерархические категории в Astra Linux (и других системах с мандатным контролем доступа — МУД) — это ключевой механизм для горизонтального разделения информации внутри одного уровня конфиденциальности. Они нужны для реализации принципа "разделения обязанностей" (Separation of Duties) и минимальных привилегий.

Если представить систему доступа в виде таблицы, где уровни (например, 1–10 — это строки (вертикальная иерархия "сверху вниз"), то неиерархические категории — это столбцы (горизонтальное разделение "по сферам деятельности"). Разряды в данном случае – это индекс, который мы задали в таблицы. Более подробно - https://wiki.astralinux.ru/pages/viewpage.action?pageId=27362553

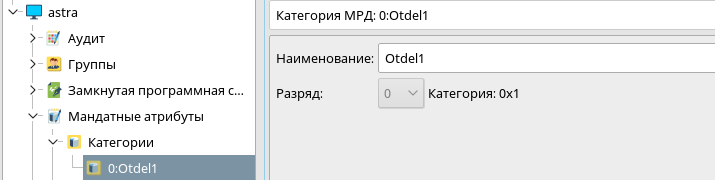


Рисунок 13 – создание новой категории

В разделе «Категории» теперь создадим новые неиерархические категории: «Otdel2» («Разряд» — 1), «Upravlenie» («Разряд» — 2). Результат представлен на рисунке 14.

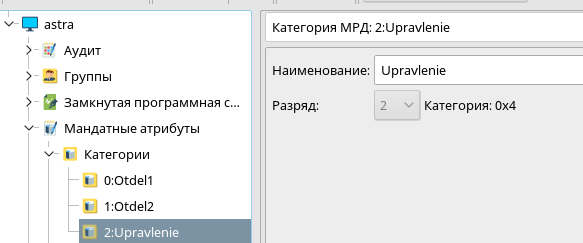


Рисунок 14 – новая неиерархическая категория

**Задание 7.** Изменить набор неиерархических категорий с использованием графической утилиты «Политика безопасности», для этого выполнить следующие действия в разделе «Категории». Выбрать неиерархическую категорию «Otdel1» и ввести наименование «Отдел\_1». Аналогично переименовать неиерархические категории «Otdel2» и «Upravlenie» в «Отдел\_2» и «Управление», соответственно.

Результат переименования представлен на рисунке 15.

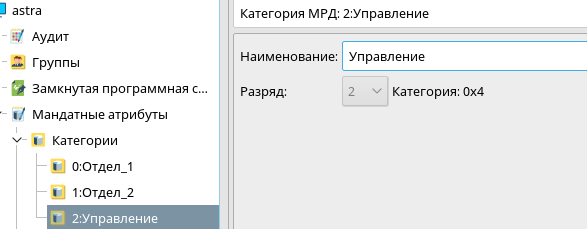


Рисунок 15 – переименование неиерархический категорий

**Задание 8.** Изменить мандатный уровень доступа с использованием графической утилиты «Политика безопасности», для этого выполнить следующие действия. Нужно создать новую группу с именем «office1» и задать первичную группу учётной записи пользователя user1 - «office1». создать новую учётную запись пользователя user0 и установить её первичную группу – «office1»; для учётной записи пользователя user2 в вкладке «МРД» выбрать максимальный уровень доступа — «Уровень\_3», максимальный набор неиерархических категорий — «Отдел\_2», после чего задать минимальный набор неиерархических категорий — «Отдел\_2»; Открыть параметры учётной записи пользователя user1 и выбрать максимальный уровень доступа — «Уровень\_3», максимальный набор неиерархических категорий — «Отдел\_1», минимальный набор неиерархических категорий — «Отдел\_1». Создать учётную запись пользователя rukoffice1 и задать первичную группу: «office1». Во вкладке «МРД» пользователя rukoffice1 выбрать максимальный уровень: «Уровень\_3», максимальный набор категорий: «Отдел\_1», «Отдел\_2», «Управление».

Для начала создадим новую группу с названием “office1” и зададим первичную группу для пользователя user1 – office1, как представлено на рисунке 16.

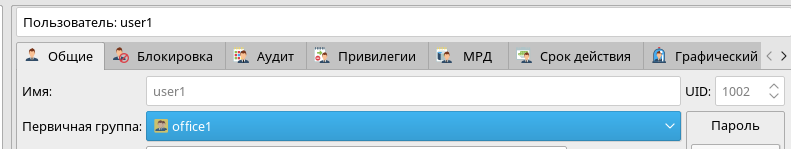


Рисунок 16 – первичная группа для пользователя user1

Создадим новую учетную запись – user0 и установим ей первичную группу – office1. В результате получится то, что представлено на рисунке 17.

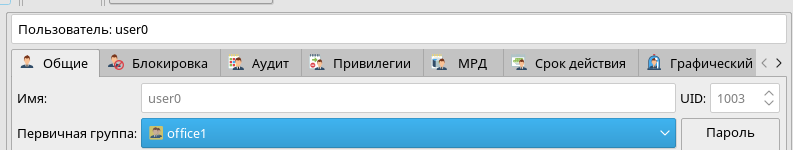


Рисунок 17 – параметры user0

Теперь выберем максимальный уровень доступа для учётной записи пользователя user0**.** Это было сделано с той целью, чтобы не создавать очередного нового пользователя.Во вкладке «МРД» нужно выбрать максимальный уровень доступа — «Уровень\_3», максимальный набор неиерархических категорий — «Отдел\_2», после чего задать минимальный набор неиерархических категорий — «Отдел\_2». В результате должно получиться то, что представлено на рисунке 18.

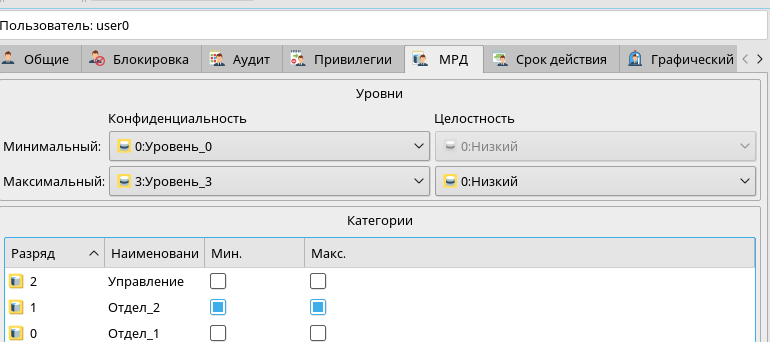


Рисунок 18 – настройки для пользователя user0

Теперь по условию задания нам нужно открыть параметры учётной записи пользователя user1 и выбрать максимальный уровень доступа — «Уровень\_3», максимальный набор неиерархических категорий — «Отдел\_1», минимальный набор неиерархических категорий — «Отдел\_1». Конфигурация представлена на рисунке 19.

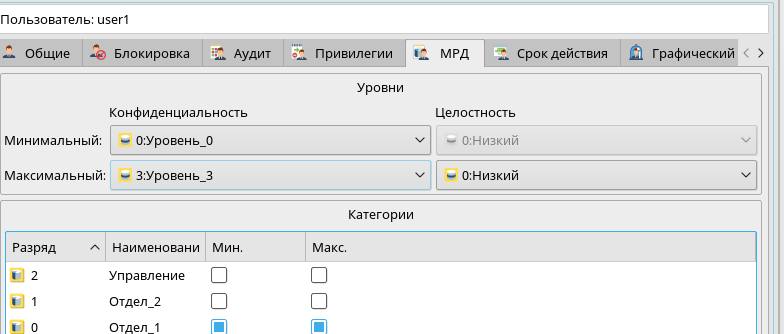


Рисунок 19 – параметры МРД для user1

Теперь создадим учётную запись пользователя rukoffice1 и выберем первичную группу: «office1». Настройка представлена на рисунке 20.

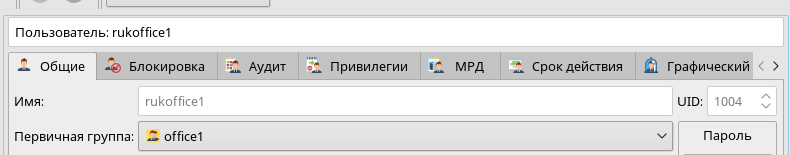


Рисунок 20 – параметры пользователя rukoffice1

Теперь во вкладке «МРД» пользователя rukoffice1 нужно выбрать максимальный уровень: «Уровень\_3», максимальный набор категорий: «Отдел\_1», «Отдел\_2», «Управление». Конфигурация представлена на рисунке 21.

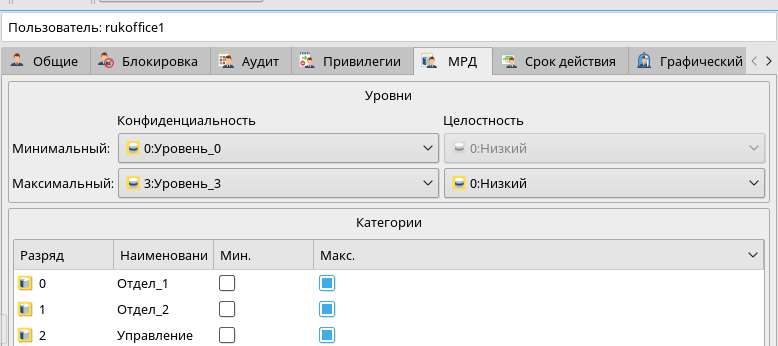


Рисунок 21 – параметры МРД для пользователя rukoffice1

**Задание 9.** Создать общий каталог для работы от имени учётных записей пользователей user1, user2, rukoffice1 в каталоге /home/work. При этом, для работы от имени учётных записей пользователей с наборами неиерархическими категорий равными «Отдел\_1», «Отдел\_2» и «Управление» выделить отдельные каталоги «otdel1», «otdel2» и «uрr» соответственно. При этом обеспечить хранение файлов с различными уровнями конфиденциальности в каталогах с использованием специального атрибута CCNR, для чего осуществить следующие действия: запустить терминал Fly в «привилегированном» режиме командой sudo fly-term. Создать каталог work и задать параметры мандатного и дискреционного управления доступом командами. создать каталог для работы от имени учётных записей пользователей с набором неиерархических категорий равным «Отдел\_1» и задать параметры мандатного и дискреционного управления доступом командами. Создать каталог для работы от имени учётных записей пользователей с набором неиерархических категорий равным «Отдел\_2» и задать параметры мандатного и дискреционного управления доступом командами. Создать каталог uрr для работы от имени учётных записей пользователей с набором неиерархических категорий равным «Управление» командами. создать вложенные каталоги Y1, Y2, YЗ в каталогах otdel1, otdel2, upr командами. Установить соответствующие владельца и группу владельца файлов. установить для каталогов otdel1, otdel2, upr необходимые уровни (см. команды для каталога upr).

Для начала откроем терминал fly в «привилегированном» режиме командой sudo fly-term. После этого у нас откроется второй терминал. Результат выполнения команды представлен на рисунке 22.



Рисунок 22 – терминал в привилегированном режиме

Теперь создадим каталог work и зададим параметры мандатного и дискреционного управления доступом командами. Команды были взяты с методического материала: mkdir /home/work, chown user1.оffice1 /home/work, chmod 750 /home/work, pdpl-file 3:0:Отдел\_1,Отдел\_2,Управление:ccnr /home/work. Результат выполнения команд представлен на рисунке 23.

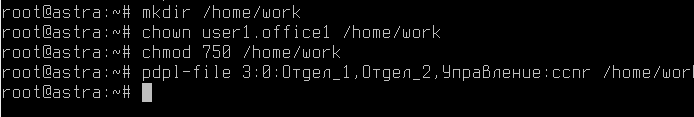


Рисунок 23 – создание каталога work и задание параметров разграничения доступа

Теперь создадим каталог для работы от имени учётных записей пользователей с набором неиерархических категорий равным «Отдел\_1» и задать параметры мандатного и дискреционного управления доступом командами. Команды: cd /home/work mkdir otdel1 chown user1:оffice1 otdel1 chmod 770 otdel1 pdpl-file 3:0:Отдел\_1:ccnr otdel1. Результат выполнения команд представлен на рисунке 24.



Рисунок 24 – создание каталога и настройка для otdel1

Теперь создадим каталог для работы от имени учётных записей пользователей с набором неиерархических категорий равным «Отдел\_2» и зададим параметры мандатного и дискреционного управления доступом командами из методического материала: mkdir otdel2 chown user2:office1 otdel2 chmod 770 otdel2 pdpl-file 3:0:Отдел\_2:ccnr otdel2. Результат выполнения представлен на рисунке 25.

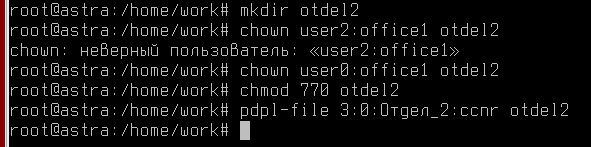


Рисунок 25 – создание каталога для “Отдел\_2”

Теперь создадим каталог uрr для работы от имени учётных записей пользователей с набором неиерархических категорий равным «Управление». Команды для выполнения: mkdir uрr chown rukoffice1:оffice1 uрr chmod 770 uрr pdpl-file 3:0:Управление:ccnr uрr. Результат выполнения представлен на рисунке 26.

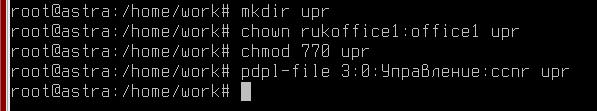


Рисунок 26 – параметры для группы Управление

Теперь создадим вложенные каталоги Y1, Y2, YЗ в каталогах otdel1, otdel2, upr командами: mkdir -p otdel1/{Y1,Y2,Y3} mkdir -p otdel2/{Y1,Y2,Y3} mkdir -p upr/{Y1,Y2,Y3}. Теперь установим соответствующие владельца и группу владельца файлов: chown user1:office1 otdel1/Y{1,2,3} chown user2:office1 otdel2/Y{1,2,3} chown rukoffice1:office1 upr/Y{1,2,3}. Результат выполнения команд представлено на рисунке 27. user0 был назначен владельцем otdel1 по ошибке.

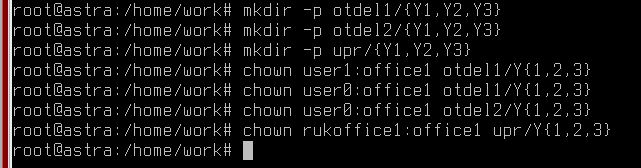


Рисунок 27 – параметры otdel1

Установить для каталогов otdel1, otdel2, upr необходимые уровни (см. команды для каталога upr). Команды для выполнения: pdpl-file 1:0:Управление:0 /home/work/upr/Y1 pdpl-file 2:0:Управление:0 /home/work/upr/Y2 pdpl-file 3:0:Управление:0 /home/work/upr/Y3 chown rukoffice1.office1 upr/Y{1,2,3} chmod 770 upr/Y{1,2,3}. Результат выполнения команды представлено на рисунке 28.

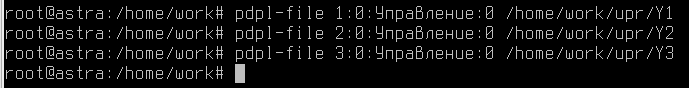


Рисунок 28 – установка необходимых уровней

Настройка Отдел1 и Отдел2 для мандатного управления представлена на рисунке 29.

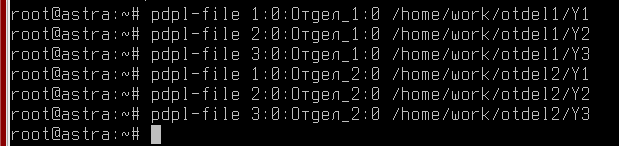


Рисунок 29 – мандатные настройки для отделов

**Задание 10.** Выполнить последовательные входы в ОССН с учётной записью пользователя user1 (неиерархическая категория — «Отдел\_1», уровни доступа 1, 2, 3). При работе на уровнях доступа 1, 2 и 3 создать в каталоге /home/work/otdel1/YX файлы с именами 11.txt, 12.txt, 13.txt соответственно, и установить дискреционные права доступа с разрешением на запись и чтение для группы оffice1 в графическом файловом менеджере Fly (fly-fm).

Зайдем для начала от лица пользователя user1 с уровнем 1. Теперь через терминал создадим файл. Файл нам видно. Результат представлен на рисунке 30.

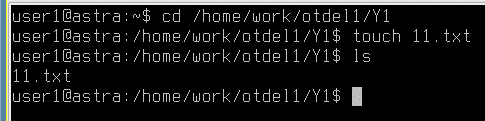


Рисунок 30 – создание файлов с уровнем 1

Теперь установим дискреционные права для файла, как представлено на рисунке 31.

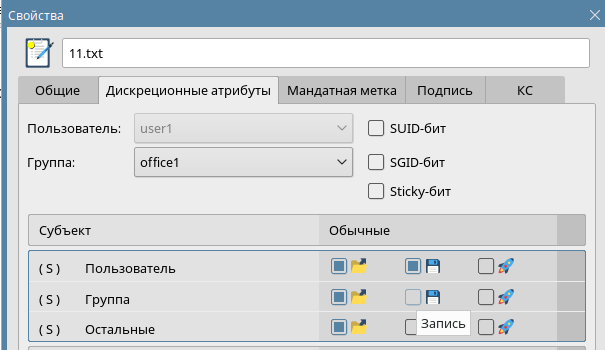


Рисунок 31 – атрибуты для файла с уровнем 1

Теперь выполним данные команды с уровнем 2. Команды аналогичные, как и на рисунке 30, только будет иное именование файла. В результате получились такие атрибуты, как представлено на рисунке 32.

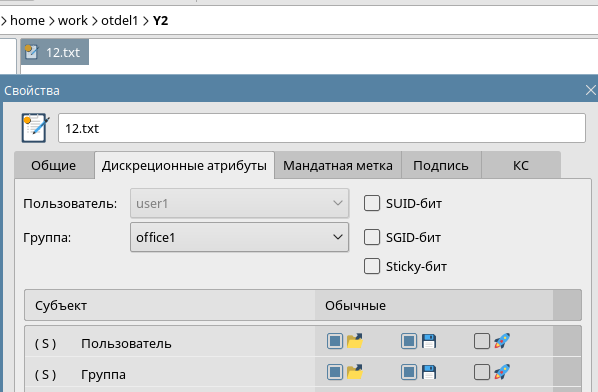


Рисунок 32 – атрибуты для файла с уровнем 2

Теперь выполнима данные команды с уровнем 3. Команды аналогичные, как и на рисунке 31, только будет иное именование файла. В результате получились такие атрибуты, как представлено на рисунке 33.

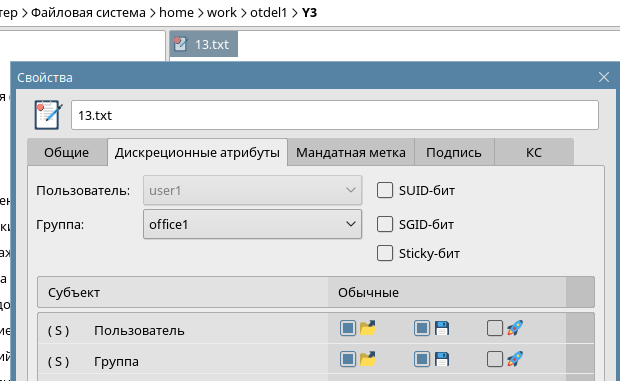


Рисунок 33 – атрибуты для уровня 3

**Задание 11.** Выполнить последовательные входы в ОССН с учётной записью пользователя usег2 (неиерархическая категория — «Отдел\_2», уровни доступа 1, 2, 3). При работе на мандатных уровнях доступа 1, 2 и 3 создать в каталоге /home/work/otdel2/YХ файлы с именами 21.txt, 22.txt, 23.txt соответственно, и установить дискреционные права доступа с разрешением на запись и чтение для группы office1 в файловом менеджере Fly (fly-fm).

Выполним теперь вход от пользователя user2. Аналогично нужно создать файл, как представлено на рисунке 30, только поменять название файла. Для уровня 1 показано на рисунке 31.

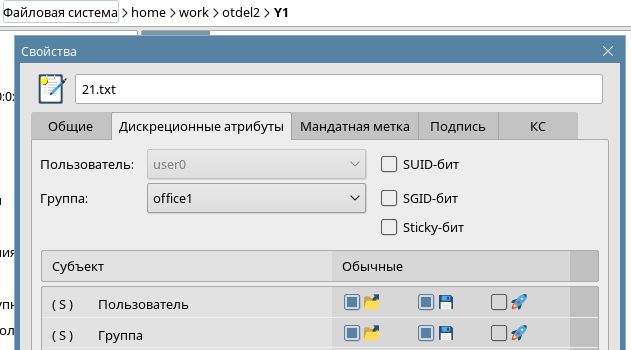


Рисунок 31 – дискреционные атрибуты

Теперь на рисунке 32 представлено, что происходит при уровне 2.

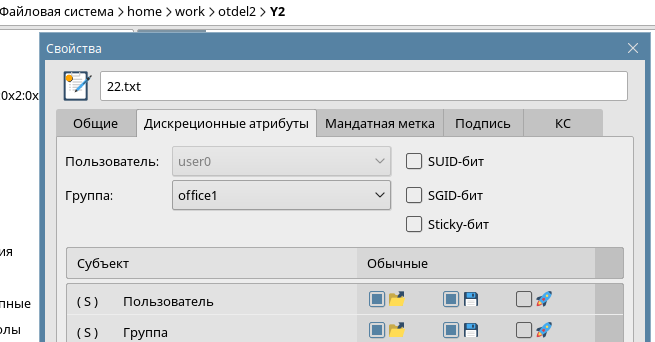


Рисунок 32 – дискреционные атрибуты

Теперь уровень 3 представлен на рисунке 33.

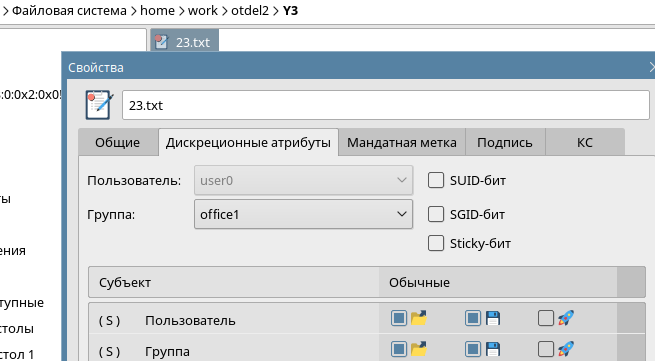


Рисунок 33 – дискреционные атрибуты

**Задание 12.** Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа - 3, неиерархическая категория — «Отдел\_2») и проверить возможность получения следующих доступов к файлам: доступ на чтение к файлам 21.txt, 22.txt, 23.txt, доступ на запись к файлу 23.txt.

Зайдем теперь под пользователем rukoffice1, выбрав уровень доступа 3 и неиерархическую категорию – отдел 2. Проверим возможность доступа к чтению, используя команды, как на рисунке 34. Есть доступ на чтение и запись к файлам 21.txt, 22.txt, 23.txt.

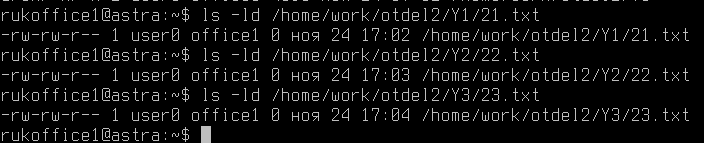


Рисунок 34 – просмотр всех файлов

**Задание 13.** Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа — 2, неиерархическая категория — «Отдел\_1») и проверить возможность получения следующих доступов к файлам: доступ на чтение к файлам 11.txt, 12.txt, доступ на запись к файлу 12.txt.

Теперь попробуем зайти от имени пользователя – rukoffice1. На рисунке 35 представлено, что у нас есть доступ и на чтение, и на запись.

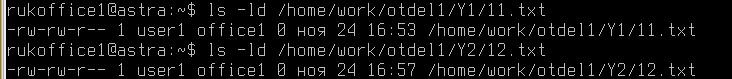


Рисунок 35 – права на чтение и т.п

**Задание 14.** Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа — 3, набор неиерархических категорий — «Отдел\_1», «Отдел\_2», «Управление») и проверить возможность получения доступа на чтение к файлам 11.txt, 12.txt, 13.txt, 21.txt, 22.txt, 23.txt.

Для всех шести файлов есть на доступ на чтение. На рисунке 36 представлен результат. Доступ на чтение есть, так как везде стоит атрибут r.

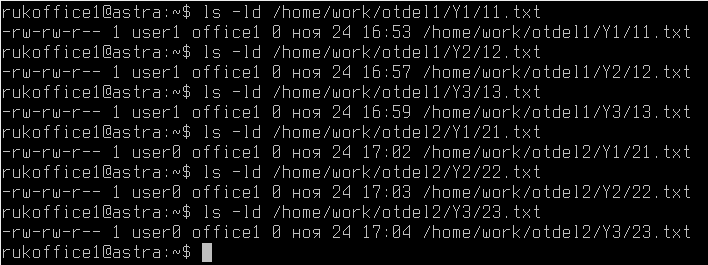


Рисунок 36 – результат просмотра всех файлов

**Задание 15.** Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа — 3, неиерархическая категория — «Управление»). Создать файл u3.txt в каталоге /home/work/uрr/Y3.

Зайдем теперь за пользователя rukoffice1 с уровнями, как представлено в условии задания. На рисунке 37 представлено создание файла u3.txt.



Рисунок 37 – файл u3.txt для задания

**Задание 16.** Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа — 3, набор неиерархических категорий: «Отдел\_1», «Отдел\_2», «Управление») и проверить возможность получения следующих доступов к файлам: доступ на запись к файлу u3.txt, доступ на чтение к файлам u3.txt, 11.txt, 12.txt, 13.txt, 21.txt, 22.txt, 23.txt. Объяснить результат.

Войдем за пользователя rukoffice1 с параметрами, которые указаны в условии задания. Проверим доступы, которые представлены на рисунке 38. У всех вышеперечисленных файлов есть доступ и на чтение, и на запись.



Рисунок 38 – параметры файлов

**Задание 17.** Для доступа к терминалу Fly настроить включение учётных записей пользователей user1, user2, rukoffice1 во вторичную группу astra-console. Это позволит данным учётным записям пользователей запускать терминал Fly с использованием комбинации Win+R.

Добавляем пользователей во вторичную группу astra-console. Конфигурация представлена на рисунке 39.

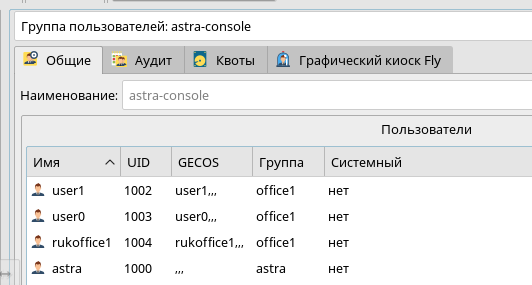


Рисунок 39 – параметры группы astra-console

**Задание 18.** Вывести в терминал Fly параметры мандатного управления доступом и мандатного контроля целостности для учётных записей пользователей. Для этого выполнить следующие действия. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа — 2, набор неиерархических категорий: «Отдел\_1», «Управление»). В терминале Fly выполнить команду pdp-id -а, проанализировать результат. Выполнить избирательный вывод параметров мандатного управления доступом (с числовыми значениями) командами pdp-id -l и pdp-id -с. Выполнить избирательный вывод параметров мандатного управления доступом (с именами) командами pdp-id -ln и pdp-id -сn.

Для начало зайдем за пользователя rukoffice1 с параметрами, как предложено по условию задания. Далее выполним команду, как предложено по условию задания. Результат на рисунке 40. В итоге у нас получилось то, что все параметры настройки входа совпадают с тем, что мы ставили при входе.

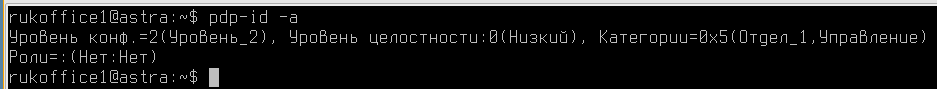


Рисунок 40 – параметры мандатного подключения

Теперь выполним избирательный вывод параметров мандатного управления доступом (с числовыми значениями) командами pdp-id -l и pdp-id -с. Результат выполнения представлен на рисунке 41.

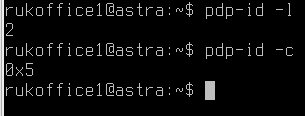


Рисунок 41 – вывод избирательный команд мандатного управления

Выполним избирательный вывод параметров мандатного управления доступом (с именами) командами pdp-id -ln и pdp-id -сn. Результат выполнения команд представлено на рисунке 42, 43. На рисунке 44 представлено все ключи для выполнения команды. Буква n добавляет буквенный вывод.



Рисунок 42 – избирательный вывод команд



Рисунок 43 – избирательный вывод команд

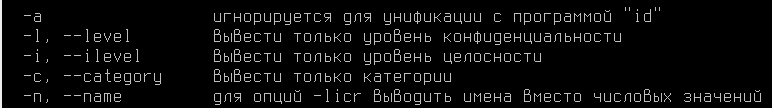


Рисунок 44 – вывод всех параметров для команд

**Задание 19.** Изменить параметры мандатного управления доступом и мандатного

контроля целостности учётной записи пользователя rukoffice1. Для этого

выполнить следующие действия. Войти в ОССН с учётной записью привилегированного пользователя (уровень доступа - 0, неиерархические категории - нет, уровень целостности - «Высокий») и запустить терминал Fly в «привилегированном» режиме командой sudo fly-term. Изменить минимальный и максимальный уровни доступа учётной записи пользователя rukoffice1 командой pdpl-user -l 0:2 rukoffice1, а также минимальный и максимальный наборы неиерархических категорий пользователя rukoffice1 командой pdpl- user -с 0:2 rukoffice1. Обнулить значения уровней доступа и наборов неиерархических категорий в параметрах учётной записи пользователя rukoffice1 командой pdpl-user -z rukoffice1. Установить значения уровней доступа и наборов неиерархических категорий в параметрах учётной записи пользователя rukoffice1 командой pdpl-user -l 1:3 -с 0:7 rukoffice1.

Для начала зайдем под пользователем – rukoffice1. Выбираем уровень доступа – 0, неиерархические категории – нет, уровень целостности – высокий. Запускаем терминал fly в привилегированном режиме, используя команду из условия задания. Изменим минимальный и максимальный уровни доступа учётной записи пользователя rukoffice1 командами из условия. На рисунке 45 показан результат применения данных команд.

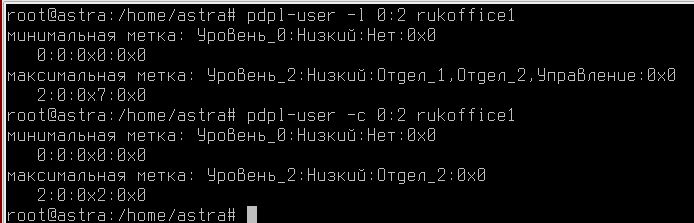


Рисунок 45 – изменение минимального и максимального уровня доступа учетной записи

Обнулим теперь значения уровней доступа и наборов неиерархический категорий в параметрах учетной записи. Команда и результат выполнения представлено на рисунке 46. Установим значения уровней доступа и наборов неиерархических категорий в параметрах учётной записи пользователя rukoffice1 командой pdpl-user -l 1:3 -с 0:7 rukoffice1, результат также представлен на рисунке 46.

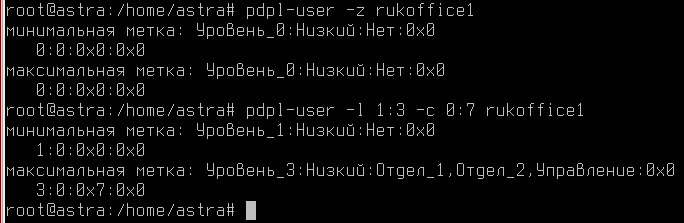


Рисунок 46 – выполнение пунктов заданий

**Задание 20.** Считать параметры мандатного управления доступом и мандатного контроля целостности учётной записи пользователя rukoffice1 из файлов настроек. Для этого выполнить следующие действия. Перейти в каталог /etc/parsec/macdb и считать минимальный и максимальный уровни доступа командами grep "rukoffice1" \* | cut -d : -f 3 и grep "rukoffice1" \* | cut -d : -f 5 соответственно. Считать минимальный и максимальный наборы неиерархических категорий командами grep "rukoffice1" \* | cut -d : -f 4 и grep "rukoffice1" \* | cut-d : -f 6 соответственно.

Для начала перейдем в директорию, как предложено по условию задания. После этого вставим команды и получим результат, который представлен на рисунках 47, 48 соответственно.



Рисунок 47 – команды по заданию

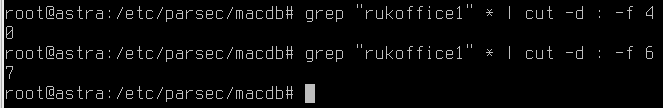


Рисунок 48 – команды по заданию

**Задание 21.** Создать и модифицировать мандатные уровни доступа, осуществив следующие действия. Вывести в терминал созданные уровни доступа командой userlev и сравнить полученные данные с настройками в утилите «Политика безопасности». добавить новый уровень доступа с именем «Уровень\_5» (значение 5) командой userlev Уровень\_5 --add 5 и вывести в терминал уровни доступа командой userlev. выполнить переименование уровня доступа «Уровень\_5» в «НовыйУровень» командой userlev Уровень\_5 — rename НовыйУровень. удалить уровень доступа с именем «НовыйУровень» командой userlev НовыйУровень --delete и вывести в терминал уровни доступа командой userlev. Выполнить переименование уровня доступа «Уровень\_4» в «НовыйУровень» командой userlev Уровень\_4 –rename НовыйУровень. Добавить возможность работы от имени учётной записи пользователя rukoffice1 на уровне доступа 4 командой pdpl-user -i 1:4 rukoffice1. выполнить попытку изменения значения уровня доступа «НовыйУровень» на 3 командой userlev НовыйУровень --modify 3, проанализировать результат. Изменить значение уровня доступа «НовыйУровень» на 5 командой userlev НовыйУровень --modify 5 и вывести в терминал максимальный уровень доступа учётной записи пользователя rukoffice1 командой pdpl-user rukoffice1, проанализировать результат. установить максимальный уровень доступа учётной записи пользователя rukoffice1 равным 5 командой pdpl-user -i 1:5 rukoffice1. Удалить уровень доступа с именем «НовыйУровень» командой userlev НовыйУровень -d и определить максимальный уровень доступа учётной записи пользователя rukoffice1 командой pdpl-user rukoffice1, проанализировать результат.

Для просмотра доступных уровней можно использовать команду, которая предложена по условию задания. В графическом интерфейсе представлены точно такие же уровни. Результат представлен на рисунке 49.

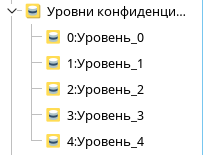
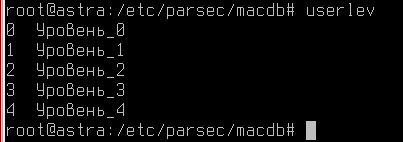


Рисунок 49 – уровни конфиденциальности

Добавим новый уровень доступа с именем «Уровень\_5» (значение 5) командой userlev Уровень\_5 --add 5 и выведем в терминал уровни доступа командой userlev. Результат представлен на рисунке 50.

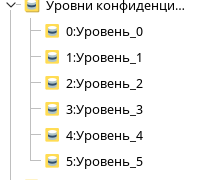
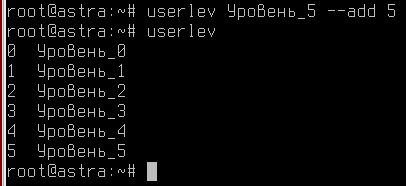


Рисунок 50 – просмотр уровней команд

Выполним переименование уровня доступа «Уровень\_5» в «НовыйУровень» командой userlev Уровень\_5 --rename НовыйУровень. Команда и результат представлены на рисунке 51.

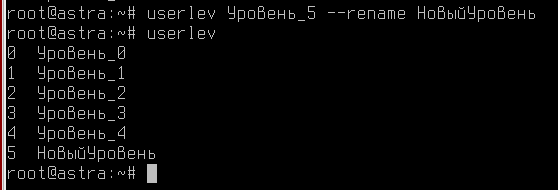


Рисунок 51 – смена уровня

Удалим уровень доступа с именем «НовыйУровень» командой userlev НовыйУровень --delete и вывести в терминал уровни доступа командой userlev. Команда и результат представлены на рисунке 52.

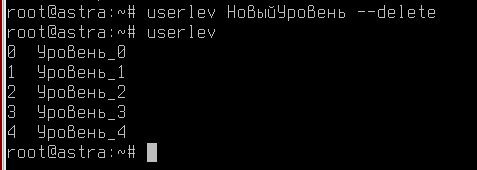


Рисунок 52 – удаление уровня

Выполним переименование уровня доступа «Уровень\_4» в «НовыйУровень» командой userlev Уровень\_4 --rename НовыйУровень. Результат представлен на рисунке 53.

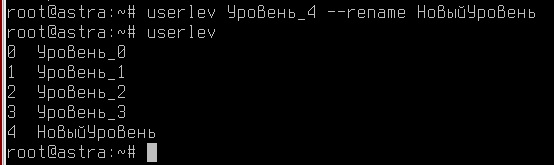


Рисунок 53 – переименование уровня

Добавить возможность работы от имени учётной записи пользователя rukoffice1 на уровне доступа 4 командой pdpl-user -i 1:4 rukoffice1. На рисунке 54 представлена команда и результат.

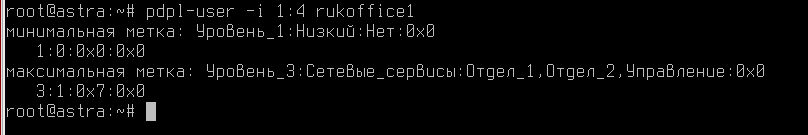


Рисунок 54 – добавление возможности работы от имени учетной записи

Выполним попытку изменения значения уровня доступа «НовыйУровень» на 3 командой userlev НовыйУровень --modify 3. Результат представлен на рисунке 55.

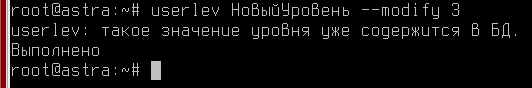


Рисунок 55 – изменение уровня

Теперь изменим значение уровня доступа «НовыйУровень» на 5 командой userlev НовыйУровень --modify 5. Выведем в терминал максимальный уровень доступа учётной записи пользователя rukoffice1 командой pdpl-user rukoffice1. Результат представлен на рисунке 56.

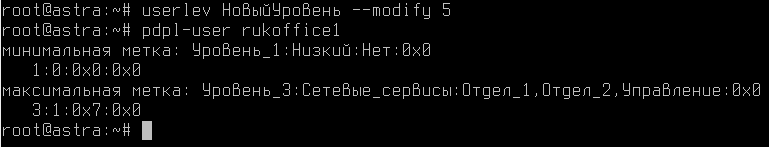


Рисунок 56 – смена уровня доступа

Установим максимальный уровень доступа учётной записи пользователя rukoffice1 равным 5 командой pdpl-user -i 1:5 rukoffice1. Результат представлен на рисунке 57.

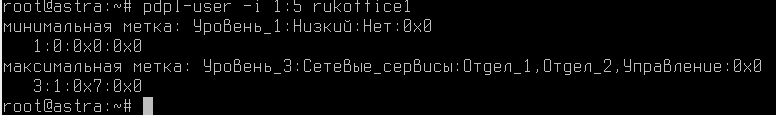


Рисунок 57 – установка максимального уровня доступа

Удалим уровень доступа с именем «НовыйУровень» командой userlev НовыйУровень -d. Определим максимальный уровень доступа учётной записи пользователя rukoffice1 командой pdpl-user rukoffice1. Результат представлен на рисунке 58.

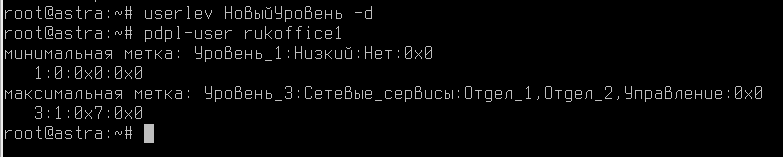


Рисунок 58 – удаление уровня доступа

Восстановим набор неиерархических категорий и уровней доступа учётной записи пользователя rukoffice1 командой pdpl-user -i 1:3 -с 0:7 rukoffice1. Команда и результат представлены на рисунке 59.

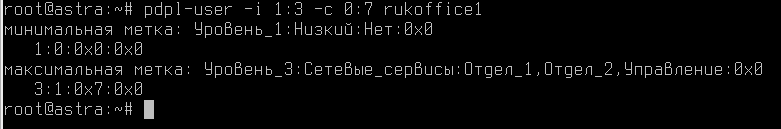


Рисунок 59 – восстановление набора неиерархических категорий

**Задание 22.** Создать и модифицировать неиерархические категории. В терминале Fly, запущенном в «привилегированном» режиме, вывести неиерархические категории командой usercat. добавить новую неиерархическую категорию командой usercat otdel3 - add 0x8. Переименовать неиерархическую категорию «otdel3» в «Отдел\_3» командой usercat otdel3 --rename Отдел\_3. Осуществить попытку модификации наборов неиерархических категорий учётной записи пользователя rukoffice1 командой pdpl-user -с 0:15 rukoffice1, проанализировать результат. добавить неиерархическую категорию «Отдел\_3» в наборы неиерархических категорий учётной записи пользователя rukoffice1 командой pdpl-user -с 3:F rukoffice1, обратить внимание на то, что неиерархическая категория задаётся в шестнадцатеричном формате. Осуществить попытку изменения значения неиерархической категории «Отдел\_3» на значение 2 командой usercat Отдел\_3 -- modify 2, проанализировать результат. изменить значение неиерархической категории «Отдел\_3» на 0x10 командой usercat Отдел\_3 --modify 10. Изменить значение неиерархической категории «Отдел\_3» на 0x20 командой usercat Отдел\_3 --modify 0x20, обратить внимание на то, что независимо от указания типа числа по префиксу «0х» (десятичное или шестнадцатеричное) значение неиерархической категории задаётся в шестнадцатеричном формате. Удалить неиерархическую категорию «Отдел\_3» командой usercat Отдел\_3 –delete. Изменить значение неиерархической категории «Управление» на 0x10 командой usercat Управление --modify 10, проанализировать результат по данным, выводимым командой pdpl-user rukoffice1. Изменить значение неиерархической категории «Управление» на 4 командой usercat Управление --modify 4.

Запустим терминал fly в привилегированном режиме и выведем неиерархические категории командой usercat. Результат выполнения команды представлен на рисунке 60.

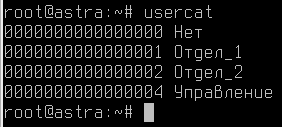


Рисунок 60 – вывод команды usercat

Добавим новую неиерархическую категорию командой usercat otdel3 --add 0x8. На рисунке 61 показан результат выполнения данной команды. Также сразу переименуем неиерархическую категорию «otdel3» в «Отдел\_3» командой usercat otdel3 --rename Отдел\_3. Результат представлен на рисунке 61.

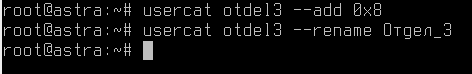


Рисунок 61 – добавление новой неиерархической категории

Осуществим попытку модификации наборов неиерархических категорий учётной записи пользователя rukoffice1 командой pdpl-user -с 0:15 rukoffice1. Команда и результат выполнения представлено на рисунке 62.

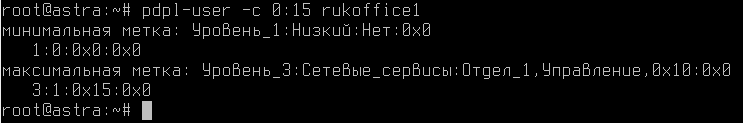


Рисунок 62 – попытка модификаций неиерархический категорий

Добавим неиерархическую категорию «Отдел\_3» в наборы неиерархических категорий учётной записи пользователя rukoffice1 командой pdpl-user -с 3:F rukoffice1. Результат выполнения команды представлен на рисунке 63.

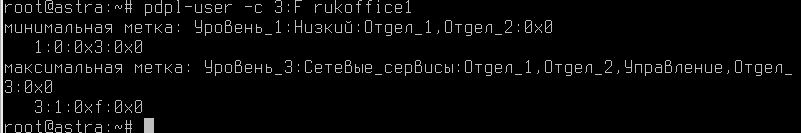


Рисунок 63 – добавление новой неиерархической категории

Осуществим попытку изменения значения неиерархической категории «Отдел\_3» на значение 2 командой usercat Отдел\_3 --modify 2, проанализировать результат.

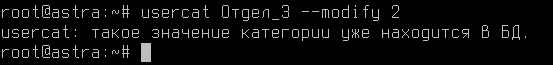


Рисунок 64 – попытка изменения неиерархической категории

Изменим значение неиерархической категории «Отдел\_3» на 0x10 командой usercat Отдел\_3 --modify 10. Результат выполнения команды представлен на рисунке 65.



Рисунок 65 – изменение неиерархической категории

Изменим значение неиерархической категории «Отдел\_3» на 0x20 командой usercat Отдел\_3 --modify 0x20. Нам нужно обратить внимание на то, что независимо от указания типа числа по префиксу «0х» (десятичное или шестнадцатеричное) значение неиерархической категории задаётся в шестнадцатеричном формате. Результат представлен на рисунке 66.



Рисунок 66 – изменение неиерархической категории Отдел3

Удалим неиерархическую категорию «Отдел\_3» командой usercat Отдел\_3 –delete. Результат представлен на рисунке 67.

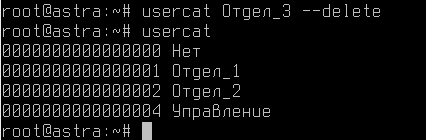


Рисунок 67 – удаление неиерархической категории

Изменим значение неиерархической категории «Управление» на 0x10 командой usercat Управление --modify 10, проанализировать результат по данным, выводимым командой pdpl-user rukoffice1. Результат представлен на рисунке 68.

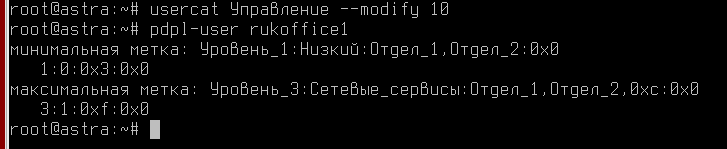


Рисунок 68 – изменение значения неиерархической категории Управление

Изменим значение неиерархической категории «Управление» на 4 командой usercat Управление --modify 4. Результат представлен на рисунке 69.

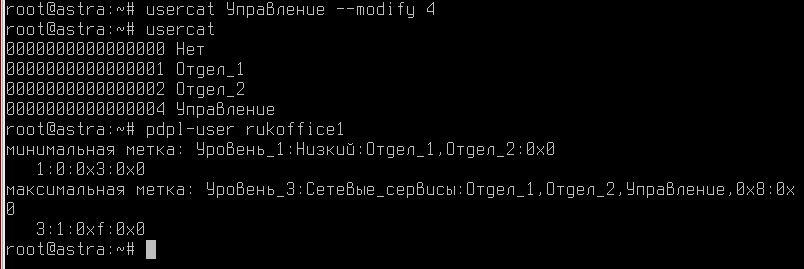


Рисунок 69 – изменение значения неиерархической категории

**Задание 23.** Для настройки привилегий учётных записей пользователей осуществить следующие действия. Вывести в терминал заданные в ОССН привилегии учётных записей пользователей командой usercaps, при работе в терминале Fly в «привилегированном» режиме. Запустить графическую утилиту «Политика безопасности» и открыть настройки учётной записи пользователя user1, в вкладке «Привилегии» установить Linux-привилегии cap\_kill, cap\_fowner и PARSЕС-привилегии parsec\_cap\_chmac, parsec\_cap\_sig, после чего закончить работу с утилитой. Вывести привилегии учётной записи пользователя user1 командой usercaps user1. В графической утилите «Политика безопасности» открыть параметры учётной записи пользователя user2, во вкладке «Привилегии» выбрать Linux-привилегии cap-kill, cap\_fowner и PARSEС-привилегии parsec\_cap\_chmac, parsec\_cap.sig. Запустить терминал Fly в «непривилегированном» режиме командой fly-term и осуществить попытку запуска команды usercaps. Определить расположение файла usercaps командой which usercaps, выполненной из «привилегированного» режима, а затем выполнить в «непривилегированном» режиме команду /usr/sbin/usercaps, проанализировать результат. Запустить терминал Fly в «привилегированном» режиме командой sudo fly-term и выполнить модификацию Linux-привилегий и РАRSЕС-привилегий командами. С использованием графической утилиты «Политика безопасности» определить установленные привилегии и формат параметра модификации привилегий учётных записей пользователей (десятичная, восьмеричная или шестнадцатеричная система счисления при этом используется?). Установить для учётной записи пользователя user1 полный список привилегий командой usercaps -f user1, затем удалить все привилегии учётной записи пользователя user1 командой usercaps -z user1. Вывести списки Linux-привилегий и PARSЕС-привилегий командами usercaps -L и usercaps -М соответственно.

Выведем в терминал заданные в ОССН привилегии учётных записей пользователей командой usercaps, при работе в терминале Fly в «привилегированном» режиме. Результат представлен на рисунке 70.

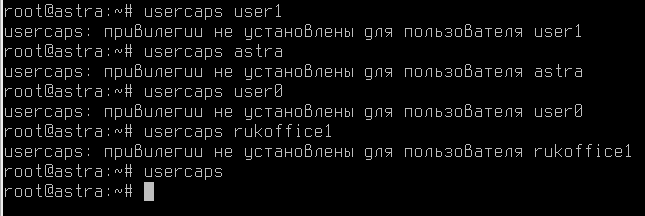


Рисунок 70 – вывод привилегий всех пользователей

Запустим графическую утилиту «Политика безопасности» и откроем настройки учётной записи пользователя user1, во вкладке «Привилегии». Нам нужно установить Linux-привилегии cap\_kill, cap\_fowner и PARSЕС-привилегии parsec\_cap\_chmac, parsec\_cap\_sig, после чего закончить работу с утилитой. Результат представлен на рисунке 71.

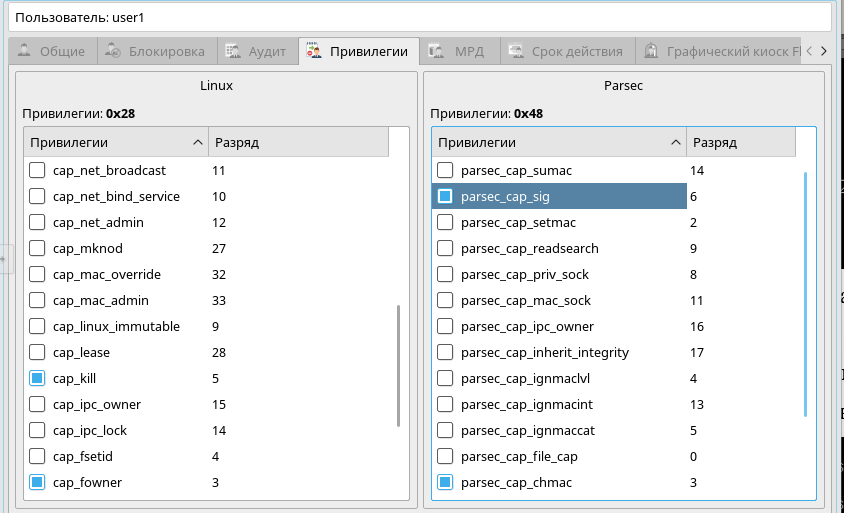


Рисунок 71 – установка Linux привилегий

Выведем привилегии учётной записи пользователя user1 командой usercaps user1. Результат представлен на рисунке 72.

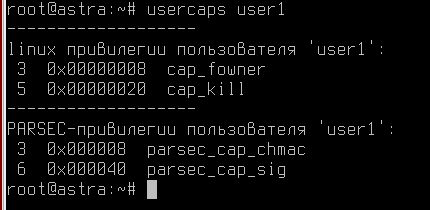


Рисунок 72 – вывод привилегий пользователя user1

В графической утилите «Политика безопасности» открыть параметры учётной записи пользователя user2, в вкладке «Привилегии» выбрать Linux-привилегии cap-kill, cap\_fowner и PARSEС-привилегии parsec\_cap\_chmac, parsec\_cap.sig. Результат настройки представлен на рисунке 73.

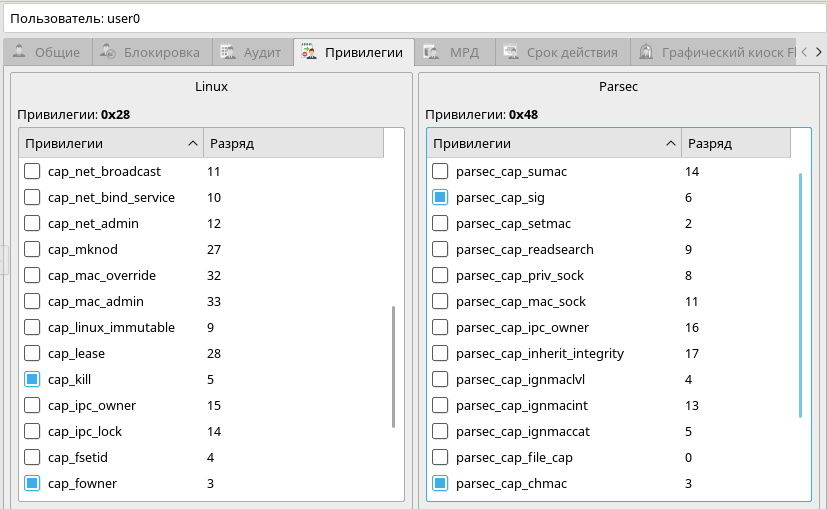


Рисунок 73 – настройка привилегий

Запустим терминал Fly в «непривилегированном» режиме командой fly-term и осуществить попытку запуска команды usercaps. В нашем случае видно, что команда не была найдена. Результат представлен на рисунке 74.

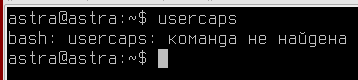


Рисунок 74 – запуск команды usercaps

Определить расположение файла usercaps командой which usercaps, выполненной из «привилегированного» режима. Результат представлен на рисунке 75.

Изображение выглядит как текст, Шрифт, снимок экрана, типография

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 75 – определение пути к файлу

Выполним в «непривилегированном» режиме команду /usr/sbin/usercaps. В результате должно получиться то, что представлено на рисунке 76.



Рисунок 76 – блокировка выполнения интерпретатором

Теперь запустим терминал Fly в «привилегированном» режиме командой sudo fly-term и выполнить модификацию Linux-привилегий и РАRSЕС-привилегий командами: usercaps -l 9 user1; usercaps -m 2 user1; usercaps -m 11 user1. Результат представлен на рисунке 77.

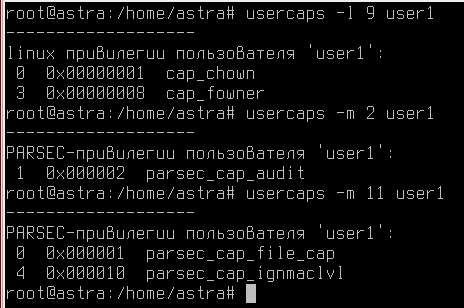


Рисунок 77 – выполним модификацию привилегий

С использованием графической утилиты «Политика безопасности» определим установленные привилегии и формат параметра модификации – 16-я система счисления. Результат представлен на рисунке 78.

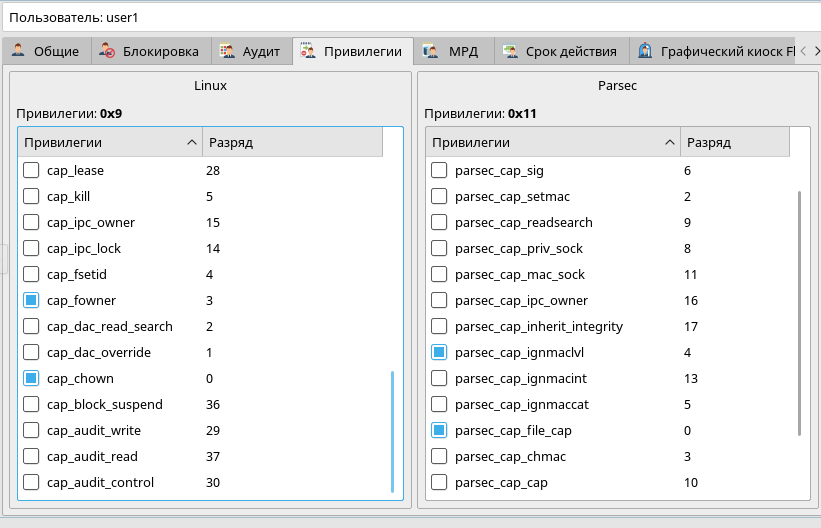


Рисунок 78 – установленные привилегии

Установим для учётной записи пользователя user1 полный список привилегий командой usercaps -f user1, а затем удалим все привилегии учётной записи пользователя user1 командой usercaps -z user1. Результат представлен на рисунке 79.

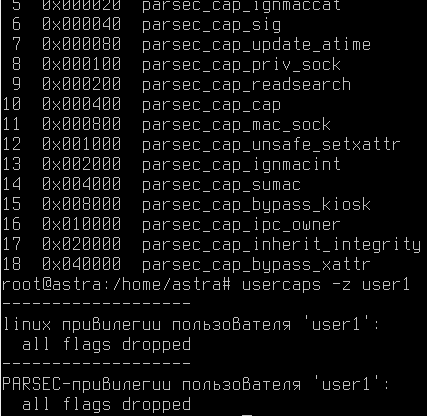
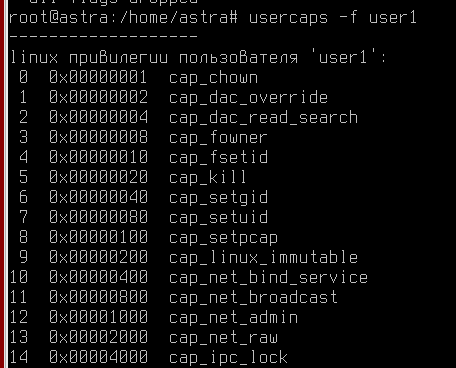


Рисунок 79 – новый список привилегий для пользователя user1

Теперь нам нужно вывести списки Linux-привилегий и PARSЕС-привилегий командами usercaps -L и usercaps -М соответственно. Результат представлен на рисунке 80, 81.

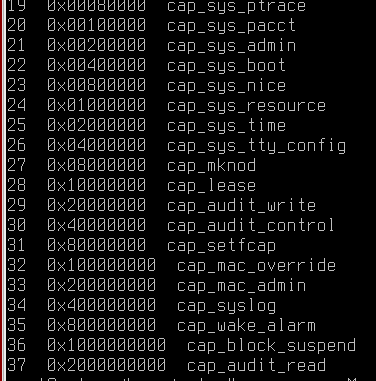
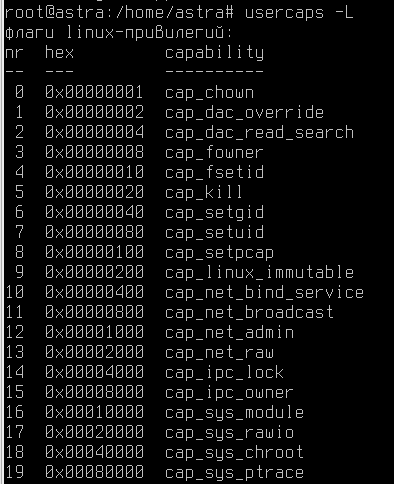


Рисунок 80 – usercaps -L

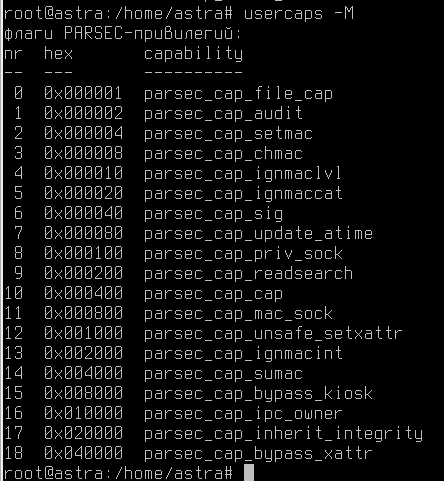


Рисунок 81 – usercaps -M

**Вывод:** в ходе лабораторной работы было изучено администрирование основных параметров мандатного управления доступом и мандатного контроля целостности в ОССН с применением графических утилит и консольных команд.

**Контрольные вопросы**

1. Какие уровни доступа и неиерархические категории создаются при установке ОССН?

В Astra Linux при установке с настроенным режимом безопасности ("смешанный" или "гарантирующий") по умолчанию создаётся набор предопределённых меток конфиденциальности.

* **Уровни доступа (иерархические)**: создаются числовые уровни от 0 до 7. Часто они ассоциируются с семантическими названиями, хотя система работает именно с числами:
  + 0 — Обычный (или Public)
  + 1 — Для служебного пользования
  + 2 — Секретно
  + 3 — Совершенно секретно
  + 4–7 — Зарезервированы для более высоких уровней.
  + **Важно:** Уровни являются иерархическими: субъект с уровнем 3 имеет доступ к информации уровней 0, 1, 2 и 3.
* **Неиерархические категории**: По умолчанию категории не создаются. Они определяются администратором безопасности в соответствии с потребностями организации (например, "ФИН", "КАДРЫ", "НИОКР"). Категории являются битовой маской, и их комбинация образует "компартмент" информации.

2. Как настроить минимальный и максимальный уровни доступа учётной записи пользователя с использованием графической утилиты fly-admin-smc?

Утилита fly-admin-smc (Graphical Interface for Security Model Control) — это графический центр управления системами защиты Astra Linux.

Запустите утилиту (требуются права администратора безопасности или root): sudo fly-admin-smc. Перейдите в раздел **"Учётные записи"**. Выберите нужного пользователя из списка и нажмите кнопку **"Изменить..."**. В открывшемся окне перейдите на вкладку **"Мандатное управление доступом"**. Найдите поля **"Минимальный уровень доступа"** и **"Максимальный уровень доступа"**. Выберите из выпадающих списков нужные значения уровней (например, мин. = 1, макс. = 3). В этом же окне вы можете назначить пользователю необходимые **неиерархические категории**, установив соответствующие флажки. Нажмите **"ОК"** для сохранения изменений.

3. Как добавить новые уровни доступа и неиерархические категории в ОССН?

**Уровни доступа**: Новые уровни (выше 7) добавляются путём редактирования конфигурационных файлов политики безопасности (например, ls-psc). **Это сложная операция, требующая пересборки политики и перезагрузки системы.** Она не выполняется в повседневной практике, так как существующего диапазона 0–7 обычно более чем достаточно. Добавление уровней — прерогатива разработчиков политики безопасности организации.

**Неиерархические категории**: добавляются относительно просто через утилиту chcc (Change Compartment Code).

4. Какие имеются особенности удаления и модификации уровней доступа и неиерархических категорий в ОССН?

* **Уровни доступа**: Модификация или удаление предопределённых уровней (0-7) **невозможна** без глубокого вмешательства в систему. Они являются основой модели безопасности.
* **Неиерархические категории**:
  + **Удаление:** Категорию можно удалить командой chcc --delete <имя\_категории>. **Однако удаление невозможно, если эта категория назначена хотя бы одному субъекту (пользователю) или объекту (файлу) в системе.** Сначала нужно убрать эту категорию у всех.
  + **Модификация:** Изменение имени категории также возможно, но требует осторожности.

5. Какие команды используются для создания, модификации и удаления уровней доступа и неиерархических категорий в ОССН?

Работа ведётся через консольные утилиты (требуют прав root или администратора безопасности).

* **Для работы с категориями (компартментами):**
  + Просмотр списка категорий: chcc --list
  + Добавление категории: sudo chcc --add <имя>
  + Удаление категории: sudo chcc --delete <имя>
  + Изменение имени категории: sudo chcc --rename <старое\_имя> <новое\_имя>
* **Для работы с уровнями доступа (метками):**
  + Просмотр текущей метки субъекта/объекта: chsl -l
  + Изменение метки файла: sudo chsl -l <уровень>[:категории] /путь/к/файлу
  + **Важно:** Прямого создания/удаления уровней через простые команды нет, как было сказано выше.

6. Какие команды используются для настройки привилегий учётных записей пользователей?

Основная команда — setplev (Set Privilege Level). Она назначает пользователю права из набора предопределённых ролей.

Просмотр текущих привилегий пользователя: setplev -l <имя\_пользователя>.

Выдача привилегий: sudo setplev <имя\_пользователя> <роль>

7. Как принудительно удалить все привилегии для заданной учётной записи пользователя?

Чтобы сбросить пользователя до роли по умолчанию (непривилегированный пользователь), используйте: sudo setplev <имя\_пользователя> user.

8. Какие существуют особенности настройки привилегий учётных записей пользователей в «непривилегированном» режиме?

**«Непривилегированный режим»** — это состояние, в котором работают обычные пользователи (роль user).

* **Ограничения:**
  1. **Запрет на понижение меток:** Пользователь не может понизить метку конфиденциальности файла или процесса. Он может только повысить её (в рамках своего диапазона доступа).
  2. **Запрет на изменение категорий:** Пользователь не может удалить категорию из метки объекта, он может только добавить категории из своего собственного набора. Например, если у файла есть категория FIN, а у пользователя есть категории FIN,HR, он может добавить к файлу категорию HR, но не может убрать FIN.
  3. **Отсутствие прав на администрирование:** Пользователь не может изменять системные настройки, управлять учётными записями, читать чужие файлы без разрешения DAC и т.д.

Настройка привилегий в таком режиме сводится не к выдаче прав, а к правильной настройке **диапазона уровней (мин./макс.)** и **набора категорий** для пользователя через fly-admin-smc или прямое редактирование БД ЛСР (что не рекомендуется).